Configurar uma sessão eBGP segura com um VTI IPsec

Contents

Introduction

Este documento descreve como proteger uma relação de vizinhança de Protocolo de Gateway de Borda Externo (eBGP - Border Gateway Protocol) com o uso de uma Interface de Túnel Virtual (VTI - Virtual Tunnel Interface) IPsec junto com as interfaces físicas (não túnel) para o tráfego de plano de dados. Os benefícios dessa configuração incluem:

- Privacidade completa da sessão vizinha do BGP com confidencialidade de dados, antirreprodução, autenticidade e integridade.
- O tráfego do plano de dados não está restrito à sobrecarga da Unidade de Transmissão Máxima (MTU - Maximum Transmission Unit) da interface de túnel. Os clientes podem enviar pacotes MTU padrão (1500 bytes) sem implicações de desempenho ou fragmentação.
- Menos sobrecarga nos roteadores de ponto final, pois a criptografia/descriptografia do Security Policy Index (SPI) é limitada ao tráfego do plano de controle BGP.

O benefício dessa configuração é que o plano de dados não está restrito à limitação da interface em túnel. Por design, o tráfego do plano de dados não é seguro para IPsec.

Prerequisites

Requirements

A Cisco recomenda que você conheça estes tópicos:

- Fundamentos de configuração e verificação do eBGP
- Manipulação do BGP Policy Accounting (PA) usando um mapa de rota
- Recursos básicos da política ISAKMP (Internet Security Association and Key Management Protocol) e IPsec

Componentes Utilizados

As informações neste documento são baseadas no Cisco IOS® Software Release 15.3(1.3)T, mas outras versões suportadas funcionam. Como a configuração de IPsec é um recurso criptográfico, certifique-se de que sua versão do código contém esse conjunto de recursos.

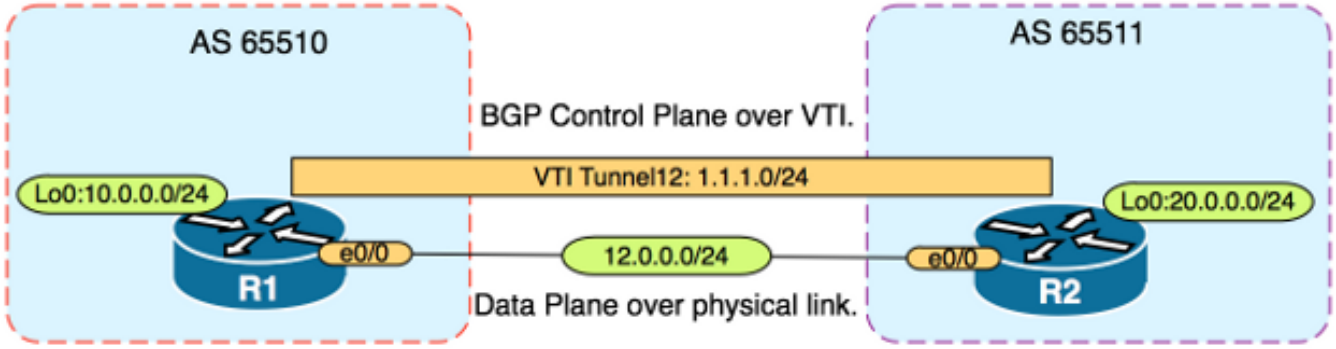
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

> **Caution**: O exemplo de configuração neste documento usa algoritmos de cifra modestos que podem ou não ser adequados ao seu ambiente. Consulte o white paper de criptografia de próxima geração para obter uma discussão sobre a segurança relativa de vários conjuntos de cifras e tamanhos de chave.

Configurar

> **Note**: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede



Configurações

Conclua estes passos:

1. Configure os parâmetros da fase 1 do Internet Key Exchange (IKE) em R1 e R2 com a chave pré-compartilhada em R1: **Note**: Nunca use os números de grupo DH 1, 2 ou 5, pois eles são considerados inferiores. Se possível, use um grupo DH com criptografia de curva elíptica (ECC) como os grupos 19, 20 ou 24. O Advanced Encryption Standard (AES) e o Secure Hash Algorithm 256 (SHA256) devem ser considerados superiores ao Data Encryption Standard (DES)/3DES e ao Message Digest 5 (MD5)/SHA1, respectivamente. Nunca use a senha "cisco" em um ambiente de produção.**Configuração do R1**

```
R1(config)#crypto isakmp policy 1
R1(config-isakmp)#encr aes
R1(config-isakmp)#hash sha256
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#group 19
R1(config-isakmp)exit
```

```
R1(config)#crypto isakmp key CISCO address 12.0.0.2
```

Configuração do R2

```
R2(config)#crypto isakmp policy 1
R2(config-isakmp)#encr aes
R2(config-isakmp)#hash sha256
R2(config-isakmp)#authentication pre-share
R2(config-isakmp)#group 19


R2(config-isakmp)exit

R2(config)#crypto isakmp key CISCO address 12.0.0.1
```

2. Configure a criptografia de senha de nível 6 para a chave pré-compartilhada na NVRAM em R1 e R2. Isso reduz a probabilidade de a chave pré-compartilhada armazenada em texto simples ser lida se um roteador for comprometido:

```
R1(config)#key config-key password-encrypt CISCOCISCO

R1(config)#password encryption aes

R2(config)#key config-key password-encrypt CISCOCISCO

R2(config)#password encryption aes
```

Note: Quando a criptografia de senha de nível 6 estiver habilitada, a configuração ativa não mostrará mais a versão em texto simples da chave pré-compartilhada:

```
!
R1#show run | include key
crypto isakmp key 6 \Nd`]dcCW\E`^WEObUKRGKIGadiAAB address 12.0.0.2

!
```

3. Configure os parâmetros da fase 2 do IKE em R1 e R2: **Configuração do R1**

```
R1(config)#crypto ipsec transform-set TRANSFORM-SET esp-aes 256 esp-sha256 ah-sha256-hmac

R1(config)#crypto ipsec profile PROFILE

R1(ipsec-profile)#set transform-set TRANSFORM-SET
R1(ipsec-profile)#set pfs group19
```

Configuração do R2

```
R2(config)#crypto ipsec transform-set TRANSFORM-SET esp-aes 256 esp-sha256 ah-sha256-hmac

R2(config)#crypto ipsec profile PROFILE

R2(ipsec-profile)#set transform-set TRANSFORM-SET

R2(ipsec-profile)#set pfs group19
```

Note: A configuração do Perfect Forward Secret (PFS) é opcional, mas melhora a força da VPN, pois força uma nova geração de chave simétrica no estabelecimento de SA da fase 2 da IKE.

4. Configure as interfaces de túnel em R1 e R2 e proteja com o perfil IPsec: **Configuração do R1**

```
R1(config)#interface tunnel 12

R1(config-if)#ip address 1.1.1.1 255.255.255.0

R1(config-if)#tunnel source Ethernet0/0

R1(config-if)#tunnel mode ipsec ipv4
```

```
R1(config-if)#tunnel destination 12.0.0.2

R1(config-if)#tunnel protection ipsec profile PROFILE
```

Configuração do R2

```
R2(config)#interface tunnel 12

R2(config-if)#ip address 1.1.1.2 255.255.255.0

R2(config-if)#tunnel source Ethernet0/0

R2(config-if)#tunnel mode ipsec ipv4

R2(config-if)#tunnel destination 12.0.0.1

R2(config-if)#tunnel protection ipsec profile PROFILE
```

5. Configure o BGP em R1 e R2 e anuncie as redes loopback0 em BGP: **Configuração do R1**

```
R1(config)#router bgp 65510

R1(config-router)#neighbor 1.1.1.2 remote-as 65511

R1(config-router)#network 10.0.0.0 mask 255.255.255.0
```

Configuração do R2

```
R2(config)#router bgp 65511

R2(config-router)#neighbor 1.1.1.1 remote-as 65510

R2(config-router)#network 20.0.0.0 mask 255.255.255.0
```

6. Configure um mapa de rota em R1 e R2 para alterar manualmente o endereço IP do próximo salto de modo que aponte para a interface física e não para o túnel. Você deve aplicar esse mapa de rota na direção de entrada. **Configuração do R1**

```
R1(config)ip prefix-list R2-NETS seq 5 permit 20.0.0.0/24

R1(config)#route-map CHANGE-NEXT-HOP permit 10

R1(config-route-map)#match ip address prefix-list R2-NETS

R1(config-route-map)#set ip next-hop 12.0.0.2

R1(config-route-map)#end

R1(config)#router bgp 65510

R1(config-router)#neighbor 1.1.1.2 route-map CHANGE-NEXT-HOP in

R1(config-router)#do clear ip bgp *

R1(config-router)#end
```

Configuração do R2

```
R2(config)#ip prefix-list R1-NETS seq 5 permit 10.0.0.0/24

R2(config)#route-map CHANGE-NEXT-HOP permit 10

R2(config-route-map)#match ip address prefix-list R1-NETS

R2(config-route-map)#set ip next-hop 12.0.0.1

R2(config-route-map)#end

R2(config)#router bgp 65511
```

```
R2(config-router)#neighbor 1.1.1.1 route-map CHANGE-NEXT-HOP in

R2(config-router)#do clear ip bgp *

R2(config-router)#end
```

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

A ferramenta Output Interpreter (exclusiva para clientes registrados) é compatível com alguns comandos de exibição.. Use a ferramenta Output Interpreter para visualizar uma análise do resultado gerado pelo comando show..

Verifique se a fase 1 do IKE e a fase 2 do IKE foram concluídas. O protocolo de linha na Virtual Tunnel Interface (VTI) não é alterado para "ativado" até que a fase 2 do IKE tenha sido concluída:

```
R1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst src state conn-id status
12.0.0.1 12.0.0.2 QM_IDLE 1002 ACTIVE
12.0.0.2 12.0.0.1 QM_IDLE 1001 ACTIVE

R1#show crypto ipsec sa | inc encaps|decaps
#pkts encaps: 88, #pkts encrypt: 88, #pkts digest: 88
#pkts decaps: 90, #pkts decrypt: 90, #pkts verify: 90
```

Observe que, antes da aplicação do mapa de rota, o endereço IP do próximo salto aponta para o endereço IP do vizinho BGP, que é a interface do túnel:

```
R1#show ip bgp
BGP table version is 2, local router ID is 10.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

Network Next Hop Metric LocPrf Weight Path
*> 20.0.0.0/24 1.1.1.2 0 0 65511 i
```

Quando o tráfego usa o túnel, o MTU é restrito ao MTU do túnel:

```
R1#ping 20.0.0.2 size 1500 df-bit
Type escape sequence to abort.
Sending 5, 1500-byte ICMP Echos to 20.0.0.2, timeout is 2 seconds:
Packet sent with the DF bit set

*May 6 08:42:07.311: ICMP: dst (20.0.0.2): frag. needed and DF set.
*May 6 08:42:09.312: ICMP: dst (20.0.0.2): frag. needed and DF set.
*May 6 08:42:11.316: ICMP: dst (20.0.0.2): frag. needed and DF set.
*May 6 08:42:13.319: ICMP: dst (20.0.0.2): frag. needed and DF set.
*May 6 08:42:15.320: ICMP: dst (20.0.0.2): frag. needed and DF set.
Success rate is 0 percent (0/5)

R1#show interfaces tunnel 12 | inc transport|line
```

```
Tunnel12 is up, line protocol is up
Tunnel protocol/transport IPSEC/IP
Tunnel transport MTU 1406 bytes <---

R1#ping 20.0.0.2 size 1406 df-bit
Type escape sequence to abort.
Sending 5, 1406-byte ICMP Echos to 20.0.0.2, timeout is 2 seconds:
Packet sent with the DF bit set
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/5/6 ms
```

Depois de aplicar o mapa de rota, o endereço IP é alterado para a interface física de R2, não para o túnel:

```
R1#show ip bgp
BGP table version is 2, local router ID is 10.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

Network Next Hop Metric LocPrf Weight Path
*> 20.0.0.0/24 12.0.0.2 0 0 65511 i
```

Altere o plano de dados para usar o próximo salto físico, ao contrário do túnel permitir MTU de tamanho padrão:

```
R1#ping 20.0.0.2 size 1500 df-bit
Type escape sequence to abort.
Sending 5, 1500-byte ICMP Echos to 20.0.0.2, timeout is 2 seconds:
Packet sent with the DF bit set
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/5 ms
```

Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.